UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/740,457	12/19/2000	Chin-Long Chen	POU920000179US1	4045

7590 05/20/2004

Lawrence D. Cutter, Attorney
IBM Corporation
Intellectual Property Law Dept.
2455 South Rd., M/S P386
Poughkeepsie, NY 12601

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	**PAPER NUMBER**
2137	6

DATE MAILED: 05/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/740,457	CHEN ET AL.	
	Examiner	Art Unit	
	Zachary A Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities:

The specification appears to contain minor typographical errors. For example, on page 3, line 1, it is assumed that "module" is intended to read "modulo". Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claim 3 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Specifically, the language of the claim raises a question as to whether the claim is directed merely to an abstract idea that is not tied to a technological art, environment, or machine which would result in a practical application producing a concrete, useful, and tangible result to for the basis of statutory subject matter under 35 U.S.C. 101. Further, the steps set forth in the claim only

comprise determining various computations, which steps are too preliminary to produce a useful result.

4. To expedite a complete examination of the instant application, Claim 3, rejected under 35 U.S.C. 101 above, is further rejected as set forth below in anticipation of applicant amending the claim to place it within the statutory categories of invention.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 1-2 and 4-6 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Specifically, the claims refer to a calculating engine that produces an output "$x\ y^{-mk}$ mod N". However, the specification does not disclose an engine with such an output, rather, it discloses a calculating engine having an output "$AB\ 2^{-mk}$ mod N", or, equivalently, "$x\ y\ 2^{-mk}$ mod N".

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 1-2 and 4-6 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Specifically, the claims refer to a calculating engine that produces an output "$x\ y^{-mk}$ mod N". However, the specification does not disclose an engine with such an output; rather, it discloses a calculating engine having an output "$AB\ 2^{-mk}$ mod N", or, equivalently, "$x\ y\ 2^{-mk}$ mod N". This contradiction renders the claims indefinite. For purposes of applying the prior art, it is assumed that the claims are intended to recite an engine having output "$x\ y\ 2^{-mk}$ mod N" as in the specification.

Particularly in reference to Claim 1, the claim is directed to a method for determining A mod N. However, it is unclear as to how performing the recited steps of operating the calculating engine, as claimed, with the recited inputs and performing the recited intervening adding step would produce the claimed result, namely A mod N.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

10. Claims 1-2 are rejected under 35 U.S.C. 102(b) as being anticipated by Tenca and Koc, "A Scalable Architecture for Montgomery Multiplication", hereinafter "Tenca".

In reference to Claim 1, Tenca discloses a method for determining A mod N as the Montgomery reduction of A (page 96, noting especially that $\bar{a} = a\ r^2\ r^{-1}$ mod M is the modular reduction of a mod M) including a calculating engine that produces an output $x\ y\ 2^{-mk}$ mod N (page 96, equation 1, noting that r is a power of 2).

Claim 2 is an apparatus claim corresponding substantially to the method of claim 1, and is rejected by a similar rationale.

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

12. Claim 3 is rejected under 35 U.S.C. 102(a) as being anticipated by Compaq Computer Corporation, "Cryptography Using Compaq MultiPrime Technology in a Parallel Processing Environment", hereinafter "Compaq".

Compaq discloses a method for determining A^B mod N where N is the product of two prime numbers N_p and N_q including determining $A_p = A$ mod N_p, $A_q = A$ mod N_q, $B_p = B$ mod $(N_p - 1)$, $B_q = B$ mod $(N_q - 1)$, $A_{pB} = (A_p)^{Bp}$ mod N_p, $A_{qB} = (A_q)^{Bq}$ mod N_p, and A^B (page 5, Figure 1, where $C=A$, $d=B$, $p=N_p$, $q=N_q$, $M=A^B$, $d_p=B_p$, $d_q=B_q$, $M_p=A_{pB}$, $M_q=A_{qB}$, and $u=U$).

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 4-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Compaq Computer Corporation, "Cryptography Using Compaq MultiPrime Technology in a Parallel Processing Environment", in view of Tenca and Koc, "A Scalable Architecture for Montgomery Multiplication".

In reference to Claims 4 and 5, Compaq discloses everything as applied to Claim 3 above. However, Compaq does not explicitly disclose using an engine with output $x\,y^{-mk} \bmod N$ in the steps of determining the modular reductions.

Tenca discloses determining a modular reduction using a calculating engine that produces an output $x\,y\,2^{-mk} \bmod N$ (page 96, equation 1, noting that r is a power of 2). Tenca also specifically discloses that these reductions are advantageous in modular exponentiation (page 96).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Compaq to use an engine with the given output in order to replace the division by N operation by a division by a power of 2 operation (see Tenca, page 94, paragraph 1) and to allow for fast and inexpensive modular multiplication for use in modular exponentiation (see Tenca, page 95, paragraph 1).

Claim 6 is an apparatus claim corresponding substantially to the method of claims 3-5, and is rejected by a similar rationale.

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Schneier, *Applied Cryptography*, discusses the Chinese remainder theorem and its use in speeding up exponentiation in public key cryptography, specifically with respect to the RSA algorithm.

b. Menezes et al, *Handbook of Applied Cryptography*, discusses an algorithm for using the Chinese remainder theorem for more efficient exponentiation.

c. Koc, Acar, and Kaliski, "Analyzing and Comparing Montgomery Multiplication Algorithms", describes a system for modular multiplication. Note especially on page 27, column 1, the use of the constant $r = 2^{sw}$ where w is the word size and s is the number of words.

d. Gressel, et al, US Patent 5742530, disclose a device for modular multiplication and exponentiation using the Montgomery method and the Chinese remainder theorem.

e. Powell, et al, US Patent 6282990, disclose a system for modular exponentiation using the Chinese remainder theorem.

f. McGinn, et al, British Patent Application 2332542, disclose a system for modular multiplication that may be used in encryption systems.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (703) 305-8902. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137